In the Claims

Please amend the claims to read as follows:

1. (original) A method of operating an integrated circuit with on-chip volatile program memory comprising: inputting a stream of data comprising unencrypted configuration data to the integrated circuit; encrypting the unencrypted configuration data using a security circuit of the integrated circuit and a security key stored in the integrated circuit; and outputting a stream of encrypted configuration data from the integrated circuit.

2. (original) The method of claim 1 wherein the stream of data is input serially.

3. (original) The method of claim 1 comprising: configuring the integrated circuit using the unencrypted configuration data.

4. (original) The method of claim 1 comprising: storing the stream of encrypted configuration data in a nonvolatile storage device.

5. (original) The method of claim 4 comprising: inputting the stream of encrypted configuration data from the nonvolatile storage device to the integrated circuit; decrypting the encrypted configuration data using the security circuit of the integrated circuit and the security key; and configuring the integrated circuit with a decrypted version of the encrypted configuration data.

6-7. (cancelled)

8. (original) The method of claim 1 comprising: generating the security key using a random number generator circuit of the integrated circuit.

9. (original) The method of claim 1 comprising: storing the security key in a device ID register of the integrated circuit.

10. (cancelled)

11. (original) The method of claim 9 wherein the ID register is nonvolatile.

12. (original) The method of claim 1 wherein the unencrypted configuration data has approximately the same number of bits as the encrypted configuration data.

13. (original) The method of claim 8 further comprising: storing the security key in a device ID register of the integrated circuit.

14-17. (cancelled)

18. (currently amended) The method of claim 9 wherein the power supply to the ID register is backed up using an external battery.

19. (original) The method of claim 1 wherein the stream of data is loaded using a JTAG interface of the integrated circuit.

20. (original) The method of claim 1 wherein the stream of data is provided using a microprocessor.

21. (currently amended) The method of claim 1 comprising: receiving the stream of unencrypted configuration data using a microprocessor.

22. (original) The method of claim 21 comprising: using the microprocessor, writing the encrypted configuration data into a nonvolatile storage device.

23. (original) The method of claim 4 wherein the nonvolatile storage device is a serial EPROM or serial EEPROM.

24. (original) The method of claim 4 wherein the nonvolatile storage device is a Flash memory.

25. (original) The method of claim 11 wherein the ID register comprises floating-gate transistors.

26. (original) The method of claim 11 wherein the ID register comprises fuses.

27. (original) The method of claim 11 wherein the ID register comprises antifuses.

28. (original) The method of claim 11 wherein the ID register is programmed during manufacture of the integrated circuit.

29. (original) The method of claim 28 wherein the ID register is programmed using a laser.

30. (currently amended) The method of claim 28 wherein the ID register is programmed using a ~~high~~ voltage high enough to substantially permanently configure a value into the ID register.

31. (original) The method of claim 18 wherein the external battery is coupled to a first power supply terminal to the ID register, and a second power supply terminal for non-backed up circuits is not coupled to the external battery.

32. (original) The method of claim 1 wherein the security key has a fixed value and further comprising: generating an initial value for the security circuit; and outputting the initial value from of the integrated circuit.

33. (original) The method of claim 32 wherein the unencrypted configuration data is encrypted using the initial value.

34. (original) The method of claim 32 wherein the initial value is generated using a random number generator.

35. (original) The method of claim 1 wherein the security circuit encrypts the unencrypted configuration data using a triple data encryption standard in a cipher block chaining mode algorithm.

36. (original) The method of claim 11 wherein the device ID register is implemented using an error correcting code scheme.

37. (original) A method of operating a integrated circuit comprising: receiving first encrypted configuration data and a first security key from a network; decrypting the first encrypted configuration data to obtain unencrypted configuration data using a first security key using user programmed circuitry of the integrated circuit; and encrypting the unencrypted configuration data using a second security key and a fixed security circuit of the integrated circuit to obtain second encrypted configuration data.

38. (original) The method of claim 37 further comprising: outputting the second encrypted configuration data from the integrated circuit.

39. (original) The method of claim 38 further comprising: storing the second encrypted configuration data in a nonvolatile storage device.

40. (original) The method of claim 39 wherein the nonvolatile storage device is a serial EPROM.

41. (original) The method of claim 37 wherein the second security key is stored in an ID register of the integrated circuit.

42. (currently amended) The method of claim 37 wherein the ~~configured user logic~~ user programmed circuitry outputs the unencrypted configuration data to the security circuit using an on-chip interconnection.

43. (original) The method of claim 37 further comprising: configuring the integrated circuit using the unencrypted configuration data.

44. (original) The method of claim 37 wherein the first encrypted configuration data is serially transferred to an I/O pin of the integrated circuit.

45. (original) The method of claim 37 wherein the security circuit encrypts the unencrypted configuration data using a triple data encryption standard (DES) in a cipher block chain (CBC) mode algorithm.

46. (original) A field programmable gate array comprising: a serial interface for loading initial configuration and key information; a battery-backed on-chip memory for storing the cryptographic key; a triple-DES encryption circuit; and an interface to an external nonvolatile memory for storing encrypted configuration data.

47. (original) A method for securely configuring an FPGA comprising: loading key information into an on-chip battery-backed register; loading an initial configuration through a JTAG interface; and storing an encrypted version of the configuration in an external nonvolatile memory.

48. (original) A field programmable gate array comprising: a plurality of static random access memory cells to store a configuration of user-configurable logic of the field programmable gate array; an ID register to store a security key; and a decryption circuit to receive and decrypt a stream of encrypted configuration data using the security key, and generate decrypted configuration data for configuring the static random access memory cells.

49. (original) The field programmable gate array of claim 48 further comprising: a first positive supply input pin coupled to the static random access memory cells, user-configurable logic, and decryption circuit; and a second positive supply input pin coupled to the ID register, wherein the second positive supply input is to be coupled to an external backup battery.

50. (original) The field programmable gate array of claim 49 wherein when power is removed from the first positive supply input pin, the configuration of the static random access memory cells is erased, and the security key stored in the ID register is maintained by the external backup battery.

51. (original) The field programmable gate array of claim 50 wherein the external backup battery only supplies power to the ID register.

52. (original) The field programmable gate array of claim 48 wherein the decryption circuit decrypts the stream of encrypted configuration data using a triple-DES algorithm.

53. (original) The field programmable gate array of claim 49 further comprising: a random number generator circuit to generate the security key.

54. (original) The field programmable gate array of claim 51 wherein a current draw on the external backup battery is about a microamp or less.

55. (original) The field programmable gate array of claim 51 wherein current draw on the external backup battery is about 10 microamps or less.

56. (new) The field programmable gate array of claim 48, further comprising:

an interface for loading configuration data; and

an interface to an external nonvolatile memory, the memory for storing the configuration data;

and wherein the ID register comprises an on-chip memory connectable to an external backup battery.

57. (new) The field programmable gate array of claim 48, further comprising an encryption circuit.

58. (new) The field programmable gate array of claim 57, wherein the decrypted configuration data is encrypted by the encryption circuit before the configuration data is passed off of the field programmable gate array.

59. (new) The method of claim 47, wherein the on-chip register is connectable to an external backup battery.

60. (new) The method of claim 59, further comprising encrypting the initial configuration using the key information.

61. (new) A field programmable gate array comprising:

an interface for loading configuration information;

an on-chip memory for storing a cryptographic key, wherein the on-chip memory is connectable to an external backup battery;

a security circuit to receive the configuration information and determine using

header information within the configuration information whether the configuration information is encrypted or unencrypted; and

an interface to an external nonvolatile memory, the memory for storing configuration data.

62. (new) The field programmable gate array of claim 61, wherein the security circuit comprises an encryption circuit for encrypting the configuration information using the cryptographic key.

63. (new) The field programmable gate array of claim 61, wherein the security circuit comprises a decryption circuit for decrypting the configuration information using the cryptographic key, if the configuration is determined to be encrypted.

64. (new) A method for securely configuring an FPGA comprising:

loading key information into an on-chip register, wherein the on-chip register is connectable to an external backup battery;

loading a configuration through an interface;

determining using header information within the configuration whether the configuration is encrypted or unencrypted;

processing the configuration using the key information; and

using the configuration information to configure the FPGA.

65. (new) The method of claim 64, wherein processing the configuration comprises decrypting the configuration if the configuration is determined to be encrypted.

66. (new) The method of claim 64, wherein processing the configuration comprises encrypting the configuration if the configuration is determined to be unencrypted.

67. (new) A field programmable gate array comprising:

a plurality of volatile memory cells to store a configuration of user-configurable logic of the field programmable gate array;

an ID register to store a security key;

a security circuit to receive a stream of configuration data and determine using

header information within the stream whether the stream is encrypted or unencrypted, and if the stream is encrypted to decrypt the stream using the security key, to generate decrypted configuration data for configuring the volatile memory cells;

a first positive supply input pin connected to the volatile memory cells, user-configurable logic, and security circuit; and

a second positive supply input pin connected to the ID register, wherein the second positive supply input is connectable to an external backup battery.

68. (new) The field programmable logic array of claim 67, wherein when power is removed from the first positive supply input pin, the configuration of the volatile memory cells is erased, and the security key stored in the ID register is maintained by the external backup battery.

69. (new) The field programmable gate array of claim 68, wherein the external backup battery only supplies power to the ID register.

70. (new) The field programmable gate array of claim 69, wherein a current draw on the external backup battery is about a microamp or less.

71. (new) The field programmable gate array of claim 69, wherein a current draw on the external backup battery is about 10 microamps or less.

72. (new) The field programmable gate array of claim 67, wherein the security circuit decrypts the stream of encrypted configuration data using a triple-DES algorithm.

73. (new) The field programmable gate array of claim 67 further comprising;

a random number generator circuit to generate the security key.

74. (new) A circuit comprising:

a field programmable gate array, comprising:

a plurality of volatile memory cells to store a configuration of user-configurable logic of the field programmable gate array;

an ID register to store a security key;

a security circuit to receive a stream of configuration data and determine using header information within the stream whether the stream is encrypted or unencrypted, and if the stream is encrypted to decrypt the stream using the security key, to generate decrypted configuration data for configuring the volatile memory cells;

a first positive supply input pin connected to the volatile memory cells, user-configurable logic, and security circuit; and

a second positive supply input pin connected to the ID register;

a power supply connected to the first positive supply input pin, to provide operating power to the volatile memory cells, user-configurable logic, and security circuit; and

a battery connected to the second positive supply input pin, to provide power to the ID register.

75. (new) The circuit of claim 74, wherein the battery provides backup power to the ID register, to maintain the security key stored in the ID register when the power supply is not active.

76. (new) The circuit of claim 74, wherein when the power supply is not active, the configuration of the volatile memory cells is erased, and the security key is maintained by the battery.

77. (new) The circuit of claim 76, wherein the battery supplies power only to the ID register.

78. (new) A method for securely configuring an FPGA using a bitstream, comprising:

loading header information contained in the bitstream into the FPGA;

determining, based on the header information, a security processing operation to apply to the bitstream;

loading configuration information contained in the bitstream into the FPGA;

applying the security processing operation to the configuration information being

loaded into the FPGA; and

using the configuration information to configure the FPGA.

79. (new) The method of claim 78, wherein the header information indicates that the configuration data is unencrypted.

80. (new) The method of claim 79, wherein the header information indicates that no security processing operation is to be applied.

81. (new) The method of claim 79, wherein the header information indicates that the security processing operation is to encrypt the unencrypted configuration information using a randomly-generated key and load the encrypted configuration information into an external non-volatile memory.

82. (new) The method of claim 79, wherein the header information indicates that the security processing operation is to encrypt the unencrypted configuration information using a key installed in the FPGA and load the encrypted configuration information into an external non-volatile memory.

83. (new) The method of claim 79, wherein the header information indicates that the security processing operation is to encrypt the unencrypted configuration information using a key included in the header information and load the encrypted configuration information into an external non-volatile memory.

84. (new) The method of claim 78, wherein the header information indicates that the configuration information is encrypted, and the security processing operation is to unencrypt the encrypted configuration data and load the unencrypted configuration information into configuration memory.

85. (new) The method of claim 78, wherein the bitstream comprises a preamble portion.

86. (new) The method of claim 85, wherein information in the preamble indicates whether the configuration information in the bitstream is encrypted or unencrypted.

87. (new) The method of claim 85, wherein based on the preamble, the integrated circuit determines whether the bitstream is for a previous version of the FPGA, without a security scheme, or the bitstream is for a version of the FPGA with the security scheme.

88. (new) The method of claim 85, wherein when using the preamble, an FPGA with a security scheme will be backwards compatible with versions of the FPGA without the security scheme.

89. (new) The method of claim 85, further comprising: when the preamble is a first value, processing the bitstream as a stream of data for a version of the FPGA without a security scheme; and when the preamble is a second value, different from the first value, processing the bitstream as a stream of configuration information for a version of the FPGA with the security scheme.

90. (new) The method of claim 78, wherein the bitstream further comprises header, initial value, configuration data, and message authentication code portions.

91. (new) A field programmable gate array, comprising:

a plurality of volatile memory cells to store a configuration of user configurable logic of the field programmable gate array;

a decryption circuit to receive and decrypt a stream of encrypted configuration data using a security key, and generate decrypted configuration data for configuring the user configurable logic;

a register to store the security key, wherein a length of the security key comprises n bits and the register comprises m bits, wherein m equals n plus k additional bits, said non-volatile register being built from unreliable memory cells;

an error-correcting code circuit which uses one or more of the k additional bits in the non-volatile register to calculate a correct value of the security key even if one or more of the m bits do not operate correctly.

92. (new) The field programmable gate array of claim 91, wherein the unreliable memory cells comprise memory cells constructed using a conventional CMOS processing flow.

93. (new) The field programmable gate array of claim 92, wherein the unreliable memory cells comprise floating gate transistors.

94. (new) The field programmable gate array of claim 91, wherein the register is connectable to a backup battery.

95. (new) The field programmable gate array of claim 91, wherein the register is a non-volatile memory.

96. (new) A field programmable gate array comprising:

user configurable logic;

a plurality of volatile memory cells to store a configuration of user configurable logic of the field programmable gate array;

a register to store a security key;

a decryption circuit to receive and decrypt a plurality of streams of encrypted configuration data using the security key, and generate decrypted configuration data for configuring the user configurable logic;

wherein each of the plurality of streams of configuration data cause an area of the field programmable gate array to be configured.

97. (new) The field programmable gate array of claim 96, wherein a subsequent one of the plurality of streams of configuration data may re-configure an area of the field programmable gate array which was previously configured by an earlier one of the plurality of streams of configuration data.

98. (new) The field programmable gate array of claim 96, wherein a single security key is used with a different initial value for each of the plurality of streams of configuration data.

99. (new) The field programmable gate array of claim 96, wherein each of the plurality of streams of configuration data can be loaded independently and verified independently of the others of the plurality of streams of configuration data.

100. (new) The field programmable gate array of claim 96, wherein the register comprises a non-volatile memory connectable to an external backup battery.

101. (new) A field programmable gate array, comprising:

a plurality of volatile memory cells to store a configuration of user configurable logic of the field programmable gate array;

a decryption circuit to receive and decrypt a stream of encrypted configuration data using a security key, and generate decrypted configuration data for configuring the user configurable logic;

a non-volatile register to store the security key;

a lock down control bit programmable to prevent the security key from being changed once the stream of configuration data is loaded.

102. (new) The field programmable gate array of claim 101, wherein the lock down control bit allows the security key to be changed if the FPGA is supplied with a key change request that includes the security key.

103. (new) A secure bitstream format, comprising:

unencrypted header information; and

configuration information;

wherein the header information specifies bitstream information to be used by a security circuit in making a security decision.

104. (new) The secure bitstream format of claim 103, wherein the configuration information is encrypted and the bitstream information specifies that the configuration information is encrypted.

105. (new) The secure bitstream format of claim 103, wherein the configuration information is unencrypted and the bitstream information specifies that the configuration information is unencrypted.

106. (new) The secure bitstream format of claim 105, wherein the bitstream information further specifies that the configuration is to be encrypted.

107. (new) The secure bitstream format of claim 103, wherein the bitstream information specifies that the bitstream is for a previous generation FPGA.

108. (new) The secure bitstream format of claim 103, wherein the security decision comprises allowing the bitstream to be loaded without performing a security action on the bitstream.

109. (new) The secure bitstream format of claim 103, wherein the security decision comprises performing a security action on the bitstream.

110. (new) The secure bitstream format of claim 109, wherein the security action comprises decrypting an encrypted bitstream.

111. (new) The secure bitstream format of claim 109, wherein the security action comprises encrypting an unencrypted bitstream.